Appendix A
Glossary of Security Acronyms and Terms

A.1 SECURITY ACRONYMS

CCP	Classified Control Point
CI	Counterintelligence
CIK	Crypto Ignition Key
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPB	Counterintelligence Programs Branch
CIVA	Counterintelligence Vulnerability Assessment
COMSEC	Communications Security
CT	Counterterrorism
DAA	Designated Approving Authority
DAS	Deputy Assistant Secretary
DCIO	Departmental Counterintelligence Official
DCIP	Departmental Counterintelligence Program
DCS	Defense Courier System
DOC	Department of Commerce
FIS	Foreign Intelligence Service
FRD	Formerly Restricted Data
GAO	General Accounting Office
IA	Information Assurance
ISOO	Information Security Oversight Office
IT	Information Technology
ITSO	Information Technology Security Officer
NATO	North Atlantic Treaty Organization

NDP	National Disclosure Policy
NIACAP	National Information Assurance Certification & Accreditation Process
NISPOM	National Industrial Security Program Operating Manual
NSA	National Security Agency
NSI	National Security Information
OADR	Originating Agency Determination Required
OCA	Original Classification Authority
RD	Restricted Data
SIMS	Security Information Management System
TA	Threat Analysis
TSCM	Technical Surveillance Countermeasures

A.2 SECURITY TERMS

Access - (1) A condition or equipment mode that allows authorized entry into a protected area without alarm by electronically or mechanically deactivating a sensor or sensors. (2) The ability and means to approach, store or retrieve data, or to communicate with or make use of a resource of an automated data processing system. (3) The ability and opportunity to obtain knowledge of classified information. An individual is considered to have access to classified information if he or she is admitted to an area where such information is kept or handled and security measures do not prevent that individual from gaining knowledge of such information.

Access Control – (1) An aspect of security that utilizes hardware systems and specialized procedures to control and monitor the movement of individuals, vehicles, or materials into, out of, or within designated areas. Access to various points may be a function of authorization level, time, or a combination of the two. (2) The use of physical security as a means of controlling movement into or out of secured areas.

Access Control System – An electronic, electro-mechanical, or mechanical system designed to identify and/or admit authorized personnel to the secure area. Identification may be based on any number of factors such as a sequencing of combinations, special keys, badges, fingerprints, signature, voice, etc. These systems are for personnel access control only and are not to be used for the protection of stored information or materials.

Accreditation – A formal declaration by a Designated Approving Authority (DAA) that a system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

ADP Facility – A facility, room, or area where computer processing and related activities occur.

Adjudication – The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance.

Agency – The "Executive agency" as defined in 5 U.S.C. § 105, and any other entity within the executive branch that comes into the possession of classified information. (E.O.12958)

Alarm Station – (1) A manually activated device installed at a fixed location to transmit an alarm signal such as a concealed holdup button in a bank teller's cage, in response to an alarm condition. (2) A well-marked emergency control unit, installed at a fixed location usually accessible to the public, used to summon help in response to an alarm condition. The control unit contains either a manually activated switch or telephone connected to fire or police headquarters, or a telephone answering service. See also remote station alarm.

Annunciator – (1) A device that signals a change of protection zone status in a security system. An annunciator may log alarms or display a continuous status for each alarm sensor in a system. Annunciators include CRT displays, sometimes called an alarm receiver, alarm monitor or alarm device. (2) The component of an alarm system that announces a change of status of the system, usually in the form of audible and/or visual signals.

Asset – Any person, facility, material, or information that has a positive value to the Department of Commerce and which is controlled by the Department of Commerce.

Astragal – A member fixed to, or a projection of, an edge of a door or window to cover the joint between the meeting of stiles to prevent access to the lock mechanism.

Balanced Magnetic Contact Switch – A two-part sensor that generates an alarm condition when a change in the magnetic field between the parts is detected. Usually mounted on a door and doorframe to detect opening of the door. A balanced magnetic contact switch provides better protection against a defeat attempt than a standard magnetic contact.

Barbed Wire – Wire, usually of 12 gauge, to which pointed barbs have been added, usually at four

inch/10.16 cm intervals. Barbed wire is often strung along the tops of fences and walls as a deterrent to entry.

Battery Backup – A standby battery that is kept fully charged for use during a primary power failure. The Battery Backup is an essential element of all electrically operated security systems.

Bolt – That part of a lock which, when actuated, is projected (or "thrown") from the lock into a retaining member, such as a strike plate, to prevent a door or window from moving or opening.

Breach – The successful defeat of security controls resulting in a penetration of the system.

Bureau – The operating units of the Department are organizational entities outside the Office of the Secretary charged with carrying out specified substantive functions (i.e. programs) of the Department (refer to DOO 1-1).

Card Access – A type of access control system that uses a card with a coded area or strip, on or inside the card, to activate a lock or other access control device. To activate the device, the card is inserted into or through a slot where the data in the coded area is read. If the code is accepted, a signal will be transmitted to unlock the device or perform some other access control function. See definition of Card Reader for more information on types.

Card Reader – A device that reads the information on a card key. Card readers may obtain data from access cards by reading punched holes, magnetic spots, stripes or wires, or any of several other methods that use punched, embossed, or embedded information. The reader may be an integral part of the lock or it can be located in the immediate vicinity. Card readers fall into one of two categories, on-line or intelligent. On-line readers must communicate with a central processor that makes the entry/exit decision and transmits a signal back to the locking device. The intelligent card reader compares the data on the card with preprogrammed parameters and entry or exit is granted or denied by the card reader itself at the reader location. Intelligent readers are also called stand-alone or off-line readers.

Central Station – (1) An organization or business established for the purpose of monitoring subscribers' alarm systems from a centralized monitoring location rather than at the individual sites. Communication with subscriber alarm systems is generally by telephone line, but may be by wireless or direct wire. The central station notifies police or fire services immediately upon receipt of an alarm. All alarms are recorded and investigated. Central stations may utilize WATS lines to extend services on a regional or national basis. (2) The control point of a monitoring system that is supervised by security personnel.

Central Station Alarm System – An alarm system that uses a central station as distinguished from a proprietary alarm system where the alarm monitoring is done on-site.

Certification – Comprehensive evaluation of the technical and non-technical security features of a system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

Change Key – A key that will operate only one lock or a group of keyed-alike locks, as distinguished from a master key. See also keyed-alike cylinders and master key system.

Classification – The act or process by which information is determined to be classified information (E.O.12958).

Classified National Security – (hereafter "classified information") Information that has been determined pursuant to E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Closed Circuit Television (CCTV) – A television system, usually hard-wired, used for proprietary purposes and not for public or general broadcast.

Combination – The group of numbers that represent the biting of a key and/or the tumblers of a lock or cylinder.

Combination Lock – A keyless lock that requires the turning of a numbered dial to a preset sequence of numbers for the lock to open. It is usually a three-position, manipulation resistant, dial-type lock, although cipher locks with push buttons are also referred to as combination locks.

Compromise – A probable compromise occurs when 1) classified material is recovered outside of a controlled area or 2) when the probable controlled area or facility is unattended and not properly secured. In either case, a compromise occurs when the material is accessible to persons who do not possess an appropriate security clearance or a need-to-know. An actual compromise occurs when with the conditions identified above, it is determined that the classified information has been released or disclosed to an unauthorized person(s) or party(ies), and that damage to national security is deemed likely or determined to have occurred as the result of this unauthorized disclosure. An actual or probable compromise of classified information constitutes a security violation. A compromise of classified information occurs whether the act was intentional or unintentional.

Confidential – The designation applied to information, the unauthorized disclosure of which reasonably

could be expected to cause damage to the National Security.

Confidential Source – Any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence (refer to E.O.12958).

Controlled Area – A specifically designated area, such as a room, office, building or facility where classified information has been authorized for handling, storage, discussion, or processing, and supplemental controls have been established which access is monitored, limited, or controlled in accordance with the DAO 207-1, Security Programs.

Cooperative Administrative Support Unit (CASU) – An organizational unit established within a multi-tenant Federal building to manage administrative services for those tenants. The tenant agencies within the building agree to establish the CASU by consolidating the various administrative functions common to most of the tenants.

Counterintelligence – Information gathered and activities conducted to protect against espionage, subversive, terrorist and/or other intelligence activities, sabotage, and assassinations conducted for, or on behalf of, foreign powers, organizations, or persons. Personnel, physical, document, and communications security programs are unrelated to counterintelligence activities and programs unless an association is established through counterintelligence functions.

Counterintelligence Community Liaison – The institution of official ties and relationships between U.S. and foreign counterintelligence organizations.

Counterintelligence Inquiries – Any investigative actions taken to determine the nature and circumstances of incidents subject to counterintelligence purview.

Counterintelligence Support to Departmental Counterterrorism and Antiterrorism Activities– Counterintelligence activities designed and conducted to identify, exploit, and neutralize real or potential threats of terrorist activities.

Counterintelligence Support to Information Systems Protection Programs – Counterintelligence activities conducted to protect Departmental information systems and the resident data from unauthorized surreptitious penetration.

Counterintelligence Vulnerability Assessment – The process for determining whether or not a

particular employee, facility, system, item of property, or Department activity is susceptible to an identified threat.

Damage to National Security – Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information (refer to E.O.12958).

Dedicated Line – (1) A power or transmissions line with a single function, such as data transmission or to a single source such as an outlet for a computer. (2) A non-shared telephone line to an individual subscriber from a central station.

Defeat – The successful unauthorized bypassing of an alarm sensor or system so that a protected area can be entered without detection.

Degausser – A device that erases magnetically encoded information from recording tapes, data disks, card keys, recording heads, and other magnetized items.

Designated Approving Authority (DAA) – An official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.

Deterrent – Any physical or psychological device or method that discourages action. In the physical security arena, locks or window grilles are physical deterrents and the presence of a guard or surveillance camera are psychological deterrents.

Disable – To temporarily or permanently place an alarm sensor or system out of service.

DOC Persons – Any organization or person, including contractors, guest researchers/scientists, experts, consultants and trainees/students, who has an on-going official association or that works directly on activities, projects, or programs of the Department of Commerce.

Economic Espionage – Foreign power-sponsored or coordinated intelligence activity directed at the U.S. Government, U.S. corporations, establishments, or persons, which involves: (1) the unlawful or clandestine targeting or acquisition of sensitive financial, trade, or economic policy information, proprietary economic information, or critical technologies, or (2) the unlawful or clandestine targeting or influencing of sensitive economic policy decisions."

Electric Eye – A detector, or detector system, which uses a photoelectric cell to trigger an alarm when the light path between it and its transmitter is interrupted.

Eligibility for Access – A favorable adjudication of an appropriate investigation of the subject's background.

Entry On Duty (EOD) – The first day that a new employee or contract employee enters employment or reports to his/her duty station for work.

Espionage – The gathering, transmitting, or losing of information respecting the national defense with the intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of a foreign nation.

Facility – A physical structure housing for assets necessary to perform a particular function, e.g., a storage facility, a meteorological facility.

Facility Code – A code used in alarm or access control equipment that identifies the customer or location of the equipment.

Fiduciary – One, such as an agent or director, that stands in a special relation of trust, confidence, or responsibility in certain obligations to others, pertaining to, or consisting of money that is not convertible into coin or specie but derives its value from public confidence or government decree; of or concerning fiat money.

Foil – An electrically conductive ribbon used for a sensing circuit. Foil is normally between .001" or .0254 mm and .003" or .0762 mm in thickness, and from .125" or 3.175 mm to 1" or 25.4 mm in width. It is most commonly used on windows and other glass applications. The metal strip, also called tape, completes an electrical circuit that, if broken, causes an alarm condition.

Foreign Contact Reporting – The acquisition, maintenance, and reporting of information concerning instances of official and unofficial contact between Department employees and non-U.S. citizens.

Foreign Government Information – Information provided to the United States Government by a foreign government or governments, an international organization of governments or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence (E.O.12958).

Foreign Intelligence Service(s) – The collective term associated with a foreign country's internal security forces and foreign intelligence collection capability. The term is used to refer to all aspects and intelligence disciplines that the service under discussion may possess.

Foreign National – TBD

Grille – A ridged screen or grate mounted over an opening to prevent entry.

Holdup Alarm – An alarm that originates from a point where holdup protection is required such as a bank teller window or store cash register. It is usually a silent alarm to protect the cashier.

Holdup Alarm System– An alarm that employs a holdup alarm device in which the signal transmission is initiated by the action of the intruder.

Infrared Motion Detector – A passive, low power, area protection device that detects a change in ambient temperature within the coverage pattern caused by the movement of a body. Sensor circuitry generates an alarm when a moving object causes a change in radiated energy levels within the coverage area. These units are more sensitive to objects moving across the beam pattern than to objects moving towards the sensor. Also called passive infrared.

Information – Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, which is owned by, produced by or for, or is under the control of the U.S. Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information. (E.O.12958).

Information Assurance (IA) – Information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

International Treaty/Agreement Support – The conduct of CI activities to protect U.S. and Departmental interests in the course of international treaties to which the Department is a U.S. participant, or when an agreement exists between the Department and a foreign entity.

Ionization Smoke Sensor – A device able to detect minute smoke particles in the air and provide early warning of a developing fire. These detectors use one or more chambers containing minuscule amounts of radioactive material that ionizes the air in the chamber. Smoke particles entering the chamber are attracted to the ionized air and the electrical balance between two electrodes is upset initiating an alarm. Most ionization smoke detectors are fail-safe in that an alarm is initiated if the sensing circuit malfunctions or power fails.

Keeper – The strike plate, mounted in a doorjamb, which receives and retains the bolt of a lock mechanism.

Key – (1) An object that carries the mechanical code configuration that unlocks a locking mechanism. (2) A system for transforming a cryptogram or cipher to plain text.

Line Supervision – A method of securing an alarm data line by introducing a continuous impedance or electronic code to the circuit. Breaking or tampering with the line initiates an alarm.

Local Alarm – An alarm that annunciates at the location of a locking device to discourage or announce intrusion attempts. The alarm usually uses a bell, siren, lighting system, or combination of such devices. It usually turns off automatically after a pre-set time, although some require a manual shutoff. A local alarm may also be linked to a central station or other remote location.

Magnetic Contact – A type of sensor that protects a moveable barrier or object such as a door or window. The device consists of two parts, mounted close together (1) the switch on the door or window frame and (2) the magnet opposite the switch on the opening portion of the door or window. In operation, when the two devices are in close proximity, the magnet holds the switch closed (or open). Separating the two halves (by opening the door or window) alters the magnetic field causing the switch to open (or close) the circuit and initiate an alarm.

National Security – The national defense or foreign relations of the United States (refer to E.O.12958).

Microwave – (1) Radio waves that have a wavelength less than 30 centimeters and operate at a frequency of 1000 MHz and higher. (2) A type of sensor that uses microwaves to detect motion. (3) A data transmission medium for alarm data.

Motion Detector – A sensor that detects movement within a protected area by comparing sequential energy transmissions or reflections, or ambient energy field levels. Motion detection systems include infrared, microwave, and ultrasonic sensors.

Multiplex Alarm System – An alarm monitoring system that multiplexes the alarm data reporting. Multiplexing is a communications mode that permits transmission of several signals on a single circuit. Multiplexing is advantageous in large security systems because considerable alarm input information can be transmitted continually without the need for extensive wiring from each sensor to the central station.

Monitor – (1) A video display unit for use with closed circuit television (CCTV). (2) A central alarm-

processing device that receives alarm signals and displays system status.

Mortise Lock – A lock with a threaded cylinder and a bolt operated by a knob or lever, designed to be recessed into the edge of a door in a cavity specifically cut out to receive it, which engages a keeper or strike plate set into the door jamb.

Need-to-Know – The determination by an authorized holder of classified information that access to the information is required by another appropriately cleared individual to perform official duties.

Nuisance Alarm – Activation of an alarm sensor by some influence for which the sensor was designed but which is not related to an intrusion attempt.

Open Storage – The storage of sensitive or classified information on shelves or in locked or unlocked non-approved containers when authorized personnel do not occupy the facility

.

Operating Unit – The operating units of the Department are organizational entities outside the Office of the Secretary charged with carrying out specified substantive functions (i.e. programs) of the Department (refer to DOO 1-1).

Original Classification – An initial determination that information requires protection against unauthorized disclosure in the interest of national security (refer to E.O.12958).

Original Classification Authority (OCA) – An individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance (refer to E.O.12958).

Panic Bar – A quick release exit bar mounted on a door to permit fast opening in a fire or panic situation. Also called a crash bar.

Photoelectric Alarm – A kind of motion detector that uses a focused beam of light (usually ultraviolet) to detect an intruder. Any interruption in the light path will set off the alarm. The beam is usually aimed so that an intruder would have to break the beam in order to move through the protected area. Sometimes called an electric eye.

Pressure Mat – A thin rubber or vinyl mat that senses intrusions designed for placement under rugs or similar floor coverings. Pressing (stepping) on the mat closes normally open built-in electrical strip switches and initiates an alarm signal. May also be used for non-security applications such as a doorbell actuator.

Program Manager – A program manager is a senior security specialist within the Office of Security who is responsible for managing a Departmental security program. The program manager's duties include providing guidance, subject matter expertise, and policy to other program mangers, security specialists, and bureau or operating unit security contacts.

Redundant – A circuit or system designed to have backup capability in the event of component or equipment failure. Redundant systems have standby components off-line and ready for automatic or manual switchover in the event of primary failure.

Remote Station – (1) A secondary or auxiliary alarm control located at some distance from the central control station. (2) A digital keypad or card reader that permits local entry/exit.

Restricted Area – A room, office, building, or facility to which access is strictly and tightly controlled. Admittance to a restricted area is limited to personnel assigned to the area or persons who have been authorized access to the area. Personnel assigned to the area must escort visitors to a restricted area and un-cleared personnel and all classified and sensitive information must be protected from observation, disclosure, or removal. The servicing security officer is authorized to designate restricted areas after appropriate security measures are in place.

Re-key – The process of modifying standard key locks or card readers to function with a new key set or facility code.

Rim Cylinder – A cylinder typically used with surface-applied locks and attached with a back plate and machine screws. It has a tailpiece to actuate the lock mechanism.

Risk Analysis – An analysis of system assets and vulnerabilities to establish an expected loss from certain events based upon estimated probabilities of the occurrence of these events. See Security Survey.

Sabotage – The willful destruction or injury of, or defective production of information, material or property of the government.

Safe – A container, usually equipped with a mounted combination lock, specifically designed for the protection of money and other highly negotiable materials or assets.

Secret – The designation applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

Secure Room – A room that offers the same or greater protection than a security container authorized for the storage of classified material, through the use of guards, alarms, or locking devices.

Security Contact – A security contact is an employee within a bureau or operating unit (non-OSY personnel and non-security specialist) whose position's secondary responsibility is to implement and administer the Department's security programs within the operating unit, for programs, projects, field sites, facilities, aircraft, or ships.

Security Hours – Hours during which a facility is not normally open for business or public access and during which more stringent access controls apply. Also called Restricted Hours or After Hours.

Security Specialist – A security specialist, as defined by OPM Standards, is a person within the GS-0080 series whose primary duties include analytical, planning, advisory, operational, or evaluative work which has as its principal purpose the development and implementation of policies, procedures, standards, training, and methods for identifying and protecting information, personnel, property, facilities, operations, or material from unauthorized disclosure, misuse, theft, assault, vandalism, espionage, sabotage, or loss. A security specialist at times is called upon to provide specialized program guidance, support, or perform compliance reviews.

Security Infraction – A security infraction occurs when classified information is not properly safeguarded in accordance with the DAO 207-1, Security Programs, but does not result in the actual or probable compromise of the material.

Security Survey – A fundamental evaluation and analysis of security-related devices, equipment, services, and procedures in use in a given location, including recommendations for security improvements. The three basic elements examined in a security survey are criticality, vulnerability, and probability. A security survey is a form of risk analysis.

Security System – A term applied to the totality of a facility's security equipment and related procedures, i.e., locks, security containers, guards, access controls, alarms, etc.

Security Vault – An area approved by the agency head, which is designed and constructed of masonry units or steel, lined construction to provide protection against forced entry. A GSA-approved modular vault may be used in lieu of the above. Vaults shall be equipped with a GSA-approved door and lock.

Security Violation – A security violation occurs when in the judgment of the investigating official,

failure to safeguard classified information could result in the actual or probable compromise of the material.

Secure Compartmented Information (SCI) – Collaterally classified information involving intelligence sources, methods, and analytical processes. In accordance with the Director of Central Intelligence, due to its sensitive nature, SCI requires limited access and strict control of its dissemination. SCI is also known as "Codeword" information.

Secure Compartmented Information Facility (SCIF) – A SCIF is an accredited area, room, group of rooms, buildings, or installation where SCI may be stored, used, discussed, and/or electronically processed.

Servicing Security Officer – A servicing security officer is a senior security specialist of the Office of Security who is stationed at either a bureau or operating unit facility or an Administrative Support Center (ASC), and is responsible for providing guidance and oversight to operating unit senior managers, program officials and security contacts on Departmental security programs and provides security administration services within their jurisdiction.

Senior Agency Official – The official designated by the agency head under section 5.6(c) of E.O. 12958 to direct and administer the agency's security program, under which information is classified, safeguarded, and declassified (E.O.12958).

Shackle – The hinged or sliding part of a padlock that does the fastening.

Slide Bolt – A simple lock that is operated by hand without using a key, a turn-piece, or other actuating mechanism. Slide bolts normally can be operated only from the side of the door on which they are mounted.

Special Agent – A special agent is an Office of Security security specialist with the authority and responsibility to perform duties conferred upon such officers in accordance with the laws of the United States and the regulations of the Department of Commerce, including the authority to investigate, administer oaths, bear firearms, and receive information on matters regarding the laws of the United States and the regulations of the Department.

Status – The condition of an alarm zone, sensor, or system at a given time.

Subversion – A systematic attempt to overthrow or undermine a government or political system by persons working secretly from within.

Surreptitious Entry – The unauthorized entry into a facility or security container in a manner in which evidence of such entry is not discernible under normal circumstances.

Surveillance – Observation or inspection of persons or premises for security purposes through alarm systems, closed circuit television (CCTV), or other monitoring methods.

Suitability Determination – Suitability refers to identifiable character traits and past conduct, which are sufficient to determine whether an individual is likely or unlikely to be able to carry out the duties of the job with appropriate efficiency and effectiveness. It also refers to statutory or regulatory bars, which prevent the lawful employment of the individual into the position.

Technical Security – The employment of specialized equipment and methods used to (1) gather information in support of counterintelligence inquiries, operations, and other activities as required, or (2) detect the presence of activities subject to counterintelligence purview.

Technical Surveillance Countermeasures – Employment of services, equipment, and techniques designed to locate, identify, and neutralize the effectiveness of technical surveillance activities.

Terrorism – The calculated use of violence or threat of violence to inculcate fear, intended to coerce or intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

Threat Analysis – Actions taken to acquire, assemble, and analyze information, which confirms or refutes the existence of known or potential danger to Department employees, information, facilities, systems, property, and activities.

Top Guard – Anti-personnel device, usually of barbed or concertina wire, installed at the tops of fences and along roof edges.

Top Secret – The designation applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

Ultrasonic – Sound waves having a frequency above that of audible sound (approximately 20,000 Hz). Ultrasonic sound is used in ultrasonic detection systems.

Unauthorized Disclosure – A communication or physical transfer of classified information to an unauthorized recipient (refer to E.O.12958).

Underwriters' Laboratories, Inc. (UL) – A nonprofit, national testing laboratory that tests and

certifies various categories of equipment and electrical devices for safety and reliability.

Vibration Detection – An alarm system which employs one or more contact microphones and vibration sensors which are fastened to the surfaces of the area or object being protected to detect excessive levels of vibration. The contact microphone system consists of microphones, a control unit containing an amplifier, an accumulator, and a power supply. The unit's sensitivity is adjustable so that ambient noises or normal vibrations will not initiate an alarm signal.

*** * * * * * ***